Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information	CC Docket No. 96-115

REPLY COMMENTS OF THE MASSACHUSETTS DEPARTMENT OF TELECOMMUNICATIONS AND CABLE

Commonwealth of Massachusetts
Department of Telecommunications and Cable

GEOFFREY G. WHY, COMMISSIONER

1000 Washington Street, Suite 820
Boston, MA 02118-6500
(617) 305-3580

Dated: July 30, 2012

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information	CC Docket No. 96-115

REPLY COMMENTS OF THE MASSACHUSETTS DEPARTMENT OF TELECOMMUNICATIONS AND CABLE

I. INTRODUCTION & SUMMARY.

The Massachusetts Department of Telecommunications and Cable (MDTC)[1] respectfully submits these reply comments to the initial comments filed on July 13, 2012 on privacy and security of information stored on mobile communications devices requested by the Federal Communications Commission (Commission) in its May 25, 2012 *CPNI Public Notice*.[2] In its *2007 Customer Proprietary Network Information (CPNI) Order*, the Commission undertook important steps toward strengthening privacy practices of telecommunications carriers.[3] In 2007, the Commission sought comment on whether to expand its CPNI rules further, specifically seeking information on the privacy of customer information stored on mobile communication

1 The MDTC is the exclusive state regulator of telecommunications and cable services within the Commonwealth of Massachusetts. MASS. GEN. LAWS ch. 25C, § 1.

2 *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, *Public Notice* (rel. May 25, 2012) ("*CPNI Public Notice*").

3 *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, *IP-Enabled Services*, WC Docket No. 04-36, *Report & Order & Further Notice of Proposed Rulemaking* (rel. Apr. 2, 2007) ("*2007 CPNI Order*").

devices.[4] Given the changes in the mobile marketplace over the past five years, the Commission now seeks to refresh the record with its *CPNI Public Notice*.[5]

In the past five years, consumers have significantly increased their usage of mobile phones in general and also their usage of smartphones which they often use for financial and other sensitive transactions.[6] Consequently, under the current regulatory framework,[7] wireless carriers have increased opportunity to collect customers' personally identifiable information, creating an increased risk of that information being distributed to third parties without customers' consent, or even knowledge.[8] Earlier this year, the Federal Trade Commission (FTC) found that "[t]he unique features of a mobile phone . . . have facilitated unprecedented levels of

---

4 *Id.*, ¶ 72.

5 *CPNI Public Notice*.

6 *See* Center for Digital Democracy Comments at 3; AARON SMITH, PEW RESEARCH CTR., 17% OF CELL PHONE OWNERS DO MOST OF THEIR ONLINE BROWSING ON THEIR PHONE, RATHER THAN A COMPUTER OR OTHER DEVICE 4 (2012), *available at* http://pewinternet.org/Reports/2012/Cell-Internet-Use-2012/Key-Findings.aspx (finding that 55 percent of cell phone owners use their phones to go online); Nielsen Wire, How US Smartphone and Tablet Owners Use Their Devices for Shopping (May 3, 2012), http://blog.nielsen.com/nielsenwire/online_mobile/how-us-smartphone-and-tablet-owners-use-their-devices-for-shopping/ (finding that 27 percent of smart phone owners use their phone to make online purchases); *In the Matter of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993; Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless, Including Commercial Mobile Services*, WT Docket 10-133, *Fifteenth Report*, ¶ 358 (rel. June 27, 2011) ("*2011 Mobile Wireless Annual Report*") ("According to one estimate, more than half of U.S. consumers, and almost 80 percent of those between the ages of 18 and 34, will use mobile financial services within five years.").

7 Senator John Kerry has noted that "the data collectors are setting the rules." Senator John Kerry, Chairman, Senate Commerce Comm., Subcomm. on Commc'ns, Tech., & the Internet, A Fair Privacy Bill of Rights for Online Consumers (May 23, 2011), *available at* http://www.kerry.senate.gov/press/speeches/speech/?id=582dfca3-5056-a032-52d5-bc0a2678c8aa ("*Senator Kerry Speech*").

8 *See* Center for Democracy & Technology Comments at 1-2; Press Release, Attorney Gen. Martha Coakley, Mass. Attorney Gen., In Recognition of National Data Privacy Day, Attorney General Coakley Advises Massachusetts Consumers to Secure Their Mobile Devices (Jan. 27, 2012), *available at* http://www.mass.gov/ago/news-and-updates/press-releases/2012/2012-01-27-data-privacy.html ("*AG Coakley Press Release*"); Press Release, Representative Edward J. Markey, U.S. House of Representatives, Markey Releases Discussion Draft of Mobile Device Privacy Act in Wake of Carrier IQ Software Concerns (Jan. 23, 2012), *available at* http://markey.house.gov/press-release/markey-releases-discussion-draft-mobile-device-privacy-act-wake-carrier-iq-software ("*Congressman Markey Press Release*") ("Consumers may have no idea that through monitoring software their mobile devices are transmitting personal information, including who is called and what is typed in text messages, to third parties . . . .").

data collection."[9] As mobile carriers collect more and more personal data, the Commission must continue to be extremely attentive to the consumer privacy practices of mobile carriers.[10]

Massachusetts has laws that address some, but not all, consumer privacy concerns.[11] And the MDTC agrees with many commenters that the Commission should act now to address recent privacy violations and security breaches,[12] as well as other issues commenters highlighted in this docket by adopting rules to enforce more adequately the duty that Congress placed upon telecommunications carriers in § 222 of the Communications Act of 1934.[13] Specifically, the Commission should: (1) implement an opt-in policy with regard to mobile carriers' sharing of customers' personal information; (2) require increased visibility, transparency, and readability of mobile carrier privacy policies and customers' options with respect to those policies; and (3) require mobile carriers to delete personal information from mobile phones if a phone is refurbished and resold.

---

9 *See* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 33 (2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf ("*2012 FTC Privacy Report*").

10 *Id.* (concluding that mobile carriers need to improve consumer privacy protections). The Commission has identified security concerns related to mobile transactions as one of the main reasons why more consumers do not participate in activities such as mobile banking. *2011 Mobile Wireless Annual Report*, ¶ 358.

11 *See* MASS. GEN. LAWS ch. 93H; 207 C.M.R. § 17.00, et seq.

12 *See, e.g., In the Matter of Annual CPNI Certification*, EB-10-TC-022, et al., *Omnibus Notice of Apparent Liability for Forfeiture and Order* (rel. Feb. 25, 2011); MASS. OFFICE OF CONSUMER AFFAIRS & BUS. REGULATION, 2011 DATA BREACH NOTIFICATIONS REPORT (2011), *available at* http://www.mass.gov/ocabr/docs/2011-data-breach-report.pdf.

13 47 U.S.C. § 222(a) ("Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers . . . ."). These comments focus on "telecommunications carriers," but the MDTC echoes commenters' note that the "mobile ecosystem" consists of numerous parties that can collect consumer information including mobile application developers and hardware manufacturers. FTC Comments at 1; Verizon Wireless Comments at 2; *2012 FTC Privacy Report* at 63.

II. BY STATUTE, MASSACHUSETTS REQUIRES MOBILE WIRELESS SERVICE PROVIDERS TO PROTECT CUSTOMER'S PRIVACY.

Massachusetts continues to be at the forefront of the fight to protect consumer privacy, imposing requirements on any company, including mobile wireless service providers, that keeps the personal information of a Massachusetts resident.[14] "Personal information" is defined as:

> "a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account . . . ."[15]

Massachusetts requires businesses or other entities owning or licensing the personal information of any Massachusetts resident to notify the Office of Consumer Affairs and Business Regulation and the Office of the Attorney General when they know of or have reason to know of a breach of security.[16] Massachusetts also requires those entities to implement a comprehensive information security program that includes, among other things, risk identification, strict employee policies,

---

[14] *See generally* MASS. GEN. LAWS ch. 93H; 207 C.M.R. § 17.00, et seq.; MASS. OFFICE OF CONSUMER AFFAIRS & BUS. REGULATION, 2011 DATA BREACH NOTIFICATIONS REPORT (2011), *available at* http://www.mass.gov/ocabr/docs/2011-data-breach-report.pdf.

[15] MASS. GEN. LAWS ch. 93H, § 1. The Commission should consider using this Massachusetts definition as a model for expanding its definition of CPNI to more fully encompass consumer personal information stored on mobile communications devices, thereby ensuring that the Commission's regulations achieve the intended result. *See* Center for Democracy & Technology Comments at 7-8 (explaining the possible limitations of the current definition of CPNI); CTIA Comments at 7 (noting that consumer information on mobile devices is not necessarily CPNI); Verizon Wireless Comments at 8.

[16] MASS. GEN. LAWS ch. 93H, § 3. "Breach of security" is defined as "the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth." *Id.* § 1. For more information, see Office of the Attorney General of Massachusetts, Guidance for Businesses of Security Breaches, http://www.mass.gov/ago/consumer-resources/consumer-information/scams-and-identity-theft/security-breaches.html (last visited July 17, 2012).

and an electronic security system.[17] The regulations require that the electronic security systems encrypt all personal information that is transmitted over public networks or wirelessly.[18]

While these laws help to prevent consumers' personal information from falling into the wrong hands and help to rectify the situation when it does, the laws do not necessarily give consumers control over if and how mobile carriers use their personal information.[19] This control has become crucial to the public interest. As the Undersecretary of the Massachusetts Office of Consumer Affairs and Business Regulation recently said:

> "There may be certain kinds of consumer behavioral information that should be off-limits to tracking and sharing. For example, should consumers be able to keep private certain behavior such as searching online for hospitals or drugs that treat cancer or finding directions on your smartphone GPS app to an appointment with your psychiatrist? The dangers of the current system are really apparent whenever we think that employers, health and life insurance companies, or total strangers can, through brokers who buy and sell tracking data, learn about personal health or social events that we consider private."[20]

The MDTC agrees with general commenters that the Commission should implement rules that would enhance consumers' control over how much of their personal information is shared, and with whom.[21] For example, the Electronic Frontier Foundation argues that consumers have a right to control their own personal data.[22] Likewise, Common Sense Media

---

17 207 C.M.R. §§ 17.03, .04.

18 *Id.* § 17.04(3).

19 *See* MASS. GEN. LAWS ch. 93H; 207 C.M.R. § 17.00, et seq.

20 Barbara Anthony, *Consumers Deserve Greater Privacy Protection While Surfing the Web*, THE CONSUMER INSIDER, June-July 2012, *available at* http://www.mass.gov/ocabr/docs/newsletters/consumerinsider2012-06.pdf.

21 *See, e.g.*, Center for Democracy & Technology Comments at 2; Electronic Privacy Information Center Comments at 9. The MDTC is aware of the Data Security and Breach Notification Act of 2012, which was recently introduced in the U.S. Senate. Data Security and Breach Notification Act of 2012, S. 3333, 112th Cong. (2d Sess. 2012). This bill would preempt state laws regarding personal data protection and notifications of breaches, including the Massachusetts regulations outlined above, replacing them with uniform, but less stringent laws. *Id.* While the MDTC sees certain advantages to a national framework for personal data protections, it is important for lawmakers and regulators alike to establish any national protections as a floor, not a ceiling. This approach will allow states like Massachusetts to make the reasoned policy decision to adopt—or preserve—increased consumer protections.

22 Electronic Frontier Foundation Comments at 2.

reasonably observes that consumers are more able to protect their personal information if they have a certain amount of control over that information.[23]

III. THE MDTC AGREES WITH COMMENTERS THAT THE COMMISSION SHOULD GIVE MOBILE WIRELESS CUSTOMERS MORE CONTROL OVER THEIR PERSONAL INFORMATION.

In the *CPNI Public Notice*, the Commission requested comment on consumers' control over their usage-related information, as well as any concerns that current mobile carrier privacy practices raise.[24] The MDTC agrees with the FTC and other commenters that under current regulations, consumers do not have sufficient control over their personal information.[25] Even if a mobile carrier must collect personal information from consumers to provide and improve[26] service, it does not mean that the carrier should have unfettered use of that information.[27] As Senator John Kerry recently observed, "[i]ndustry self-regulation, though improved under the pressure of agency and policymaker advocacy, remains inadequate and can only cover those who volunteer to participate, not all collectors of our personal information."[28] The Commission should heed this observation and implement rules that sufficiently protect consumers' rights to keep their personal information from being disbursed or used without their express permission, and to know how carriers would use that information should the customer assent to such use.[29]

---

23 Common Sense Media Comments at 3.

24 *CPNI Public Notice* at 4.

25 *See* FTC Comments at 2; Center for Democracy & Technology Comments at 2; Electronic Privacy Information Center Comments at 9.

26 *See* Sprint Nextel Comments at 6.

27 *See Senator Kerry Speech*.

28 *The Need for Privacy Protections: Is Industry Self-Regulation Adequate?: Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 112th Cong. (2d Sess. 2012) (statement of Sen. John Kerry, Chairman, Subcomm. on Commc'ns, Tech., & the Internet, S. Comm. on Commerce, Sci., & Transp.); *see also* Center for Digital Democracy Comments at 11.

29 *2012 FTC Privacy Report* at 73.

A. Commenters Urge The Commission To Require Mobile Carriers To Obtain Affirmative Customer Consent Prior To Sharing The Customer's Personal Information With Third Parties.

The MDTC agrees with numerous commenters who argue that the Commission should alter its current rule regarding consumers' control over their own CPNI and require mobile carriers to implement an opt-in policy.[30] The Commission's rules currently allow for an opt-out policy, permitting carriers to use and disclose to third parties customers' personal information as long as the customers have not stated that they do not wish their information be disseminated.[31] This means that customers, if unaware of their mobile carrier's privacy policy and consequently their right to opt-out, may find their personal information in the hands of not only their carrier, but also third parties to which the carrier has sold the information.[32]

In 2009, the FTC suggested four principles regarding consumers' personal information for companies engaged in online advertising.[33] One of these recommendations was that a company should obtain affirmative consent from consumers before using their sensitive data for behavioral advertising.[34] Given the increased privacy risks in the current mobile phone market—even since the FTC's 2009 report—the FCC should take this opportunity to put the FTC's recommendation into practice and apply this principle in amending its privacy regulations for mobile wireless carriers.

---

30 *See, e.g.*, Electronic Privacy Information Center Comments at 9-10; Common Sense Media Comments at 2; New America Foundation, et al. Comments at 8-12.

31 47 C.F.R. § 64.2007.

32 *See Congressman Markey Press Release*.

33 FTC, FTC STAFF REPORT: SELF REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVER. 45-47 (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf ("*FTC Online Advertising Report*") (highlighting transparency and consumer control, reasonable security and limited data retention for consumer data, affirmative express consent for material changes to existing privacy promises, and affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising). The MDTC recommends that the Commission take these principles into account before making any rule changes regarding personal information.

34 *Id.* at 47.

Mobile customers often pay little to no attention to the privacy policies of their mobile carriers.[35] The MDTC recently noted in its June 25, 2012 *Cramming Comments* that third party billing disclosures are "simply [] one of the documents a consumer will be asked to sign in the avalanche of paperwork a consumer is provided at the point-of-sale."[36] The same principle applies to an opt-out policy regarding a consumer's personal information.[37] When consumers sign up for a new mobile phone they are given all sorts of forms, warranties, manuals, etc. and understandably may not take the time to read every document and disclosure with which they are presented.[38] Empowering consumers by bringing explicitly the issue of personal information sharing to their attention and allowing them to decide if, how, and when carriers distribute their personal information is an important step toward protecting consumer privacy that the Commission should take.

The parent companies of two major mobile carriers in the United States, while not speaking specifically on the privacy practices of their mobile carrier subsidiaries, testified before Congress in support of requiring customers to affirmatively opt-in before a company can collect their personal information for behavioral advertising purposes.[39] The MDTC agrees with this approach and with many commenters that the Commission should empower consumers by eliminating mobile carriers' current option for an opt-out policy.[40] Rather, the Commission

---

35 *See* Electronic Frontier Foundation Comments at 5; New America Foundation, et al. Comments at 9; *cf. In the Matter of Empowering Consumers to Prevent and Detect Billing for Unauthorized Charges ("Cramming"); Consumer Information and Disclosure; Truth-in-Billing and Billing Format*, CG Docket Nos. 11-116, 09-158, CC Docket No. 98-170, *MDTC Comments* at 8-9 (filed June 25, 2012) ("*MDTC Cramming Comments*").

36 *MDTC Cramming Comments* at 8.

37 Electronic Privacy Information Center Comments at 13.

38 *Id.*

39 *Broadband Providers and Consumer Privacy: Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 110th Cong. 5, 12 (2008) (statements of Dorothy Attwood, Senior Vice President Public Policy and Chief Privacy Officer, AT&T Services, Inc. and Thomas J. Tauke, Executive Vice President, Public Affairs, Policy and Communications, Verizon Communications, Inc.).

40 *See, e.g.*, Electronic Privacy Information Center Comments at 9-10; Common Sense Media Comments at 2; New America Foundation, et al. Comments at 8-12.

should implement a mandatory opt-in policy, thereby requiring consumers to affirmatively choose to give their mobile carrier the right to share their personal information with third parties.[41] Under an opt-in approach consumers will have more control over their personal information.

B. The Commission Should Continue To Ensure That Consumers Can Read And Understand Disclosures Regarding Their Personal Information.

Regardless of whether the Commission adopts a comprehensive opt-in policy for mobile carriers' sharing of personal information, the MDTC agrees with commenters that it is imperative that the Commission continues to ensure that mobile service providers clearly and conspicuously disclose their privacy disclosures to customers.[42] Regarding privacy disclosures, the FTC called for disclosures that are "clear, concise, consumer-friendly, and prominent . . ."[43] and subsequently called on companies to develop "short, meaningful disclosures."[44] The Commission's current rules requiring certain notice to consumers are a good starting point and the Commission should preserve each of these currently required disclosures.[45] In addition, however, commenters are correct in finding that the Commission should require mobile carriers to provide at the point-of-sale[46] a conspicuous and concise statement highlighting consumers' rights and options regarding the use of their personal information.[47]

---

41 *See* 47 C.F.R. § 64.2003(k) (defining "Opt-in approval").

42 *See* FTC Comments at 3; Center for Democracy and Technology Comments at 6. The Massachusetts Attorney General has specifically defined "clear and conspicuous" in terms of disclosures for retail advertisements. 940 C.M.R. § 6.01.

43 *FTC Online Advertising Report* at 46.

44 *2012 FTC Privacy Report* at 13.

45 *See* 47 C.F.R. § 64.2008(c).

46 In addition to privacy concerns regarding personal information that mobile carriers collect, the Commission should also take into account mobile device applications ("apps"). Apps are ubiquitous on smartphones and despite the frequent practice of apps collecting consumers' personal information, many apps do not even include a privacy disclosure upon download. *2012 FTC Privacy Report* at 11; *see also Multistakeholder Process To Develop Consumer Data Privacy Codes of Conduct*, 70 Fed. Reg. 13098, 13099 (Mar. 5, 2012). This is an area of mobile communications privacy that is growing in importance and concern, and is one that warrants the Commission's attention. *See Multistakeholder Process To Develop*

Many consumers do not realize that their service provider has the ability to disclose personal data to third parties. Frequently and by practice, many consumers put passwords on their smartphones because they do not want others to be able to see the personal information that they save on their phones.[48] One of the few differences between the personal information visible directly on a mobile phone and the personal information that a carrier collects and shares with third parties is that consumers know that there is sensitive personal data physically accessible on their smartphones. Often, however, those same consumers have no idea that their carriers are collecting and selling that same data, as well as even more sensitive data, remotely.[49] As noted above, consumers are given pages of documents upon signing up for a new mobile phone. Many consumers skim through these pages or do not look at them at all.[50] Others that do read the disclosures often do not understand what they are reading.[51] An issue as important as consumer privacy should not be buried in a pile of documents. Rather, the highlights of any disclosures, policies, or consumer options related to a consumer's personal information should be noticeable, readable, and sufficiently succinct to capture consumers' attention.[52] Accordingly, the Commission should require that carriers bring a concise version of the highlights of their privacy

---

Consumer Data Privacy Codes of Conduct, NTIA Docket No. 120214135–2135–01, *World Privacy Forum Comments* at 4; *Future of Privacy Forum Comments* at 5-8.

47 *See* Electronic Frontier Foundation Comments at 3; Electronic Privacy Information Center Comments at 9. For a list of considerations in evaluating whether a disclosure is sufficiently clear and conspicuous, see FTC, DOT COM DISCLOSURES: INFO. ABOUT ONLINE ADVER. 5-6 (2000), *available at* http://www.ftc.gov/os/2000/05/0005dotcomstaffreport.pdf.

48 *See AG Coakley Press Release*.

49 *Congressman Markey Press Release*; *2012 FTC Privacy Report* at 33 (noting that despite consumers freely giving up personal information through the use of their mobile phones, they often do not know that the information is being collected).

50 *See 2012 FTC Privacy Report* at 61 (finding that most companies' privacy policies are ineffective because they are, among other things, too long). The FCC also may want to consider, to the extent possible, adopting standard privacy disclosures for mobile carriers. Different mobile carriers have different privacy disclosures, creating the potential for even more consumer confusion. *See* MOBILE MARKETING ASSOCIATION, U.S. CONSUMER BEST PRACTICES (v. 6.1 2011), *available at* http://www.mmaglobal.com/uploads/Consumer-Best-Practices.pdf.

51 *2012 FTC Privacy Report* at 35; *MDTC Cramming Comments* at 8 ("Consumers may not be able to make informed decisions if the disclosure language is too complex, in small font, or too lengthy.").

52 *2012 FTC Privacy Report* at 35 (concluding that many consumers do not understand companies' privacy practices).

policies—whether clearly visible on paper, orally, or both—to the consumer's direct attention. Emphasizing these critical policies will help consumers manage their private personal data contained on their mobile devices.

C. The Commission Should Require Mobile Carriers To Delete All Personal Information From Refurbished And Resold Phones.

In addition to requiring an opt-in policy and more comprehensible, conspicuous disclosures, the Commission should require mobile carriers to erase all consumer information from a wireless device before the carrier resells the device to another customer. Any protections suggested above that the Commission adopts will, at best, only prevent mobile carriers from disbursing the information that they collect as part of their business relationship with the customer. These types of protections will do nothing to prevent third parties from taking and using personal information stored directly on mobile phones.

When a mobile carrier refurbishes and resells a phone, the prior owner's information still may be on the physical device and end up in the hands of the new owner. The Mobile Marketing Association's U.S. Consumer Best Practices includes a provision designed "to ensure that mobile content programs subscribed to by previous holders of a specific phone number do not continue to be delivered or billed to a subsequent holder of that number when it is reassigned."[53] The FCC should build on this provision and require that mobile carriers delete all personal information when they refurbish and resell a mobile phone to a new user.

D. The Commission Should Work With Other Federal And State Agencies To Arrive At The Best Solution For Consumers.

Finally, interagency collaboration in this area of consumer protection would benefit all parties. As a variety of commenters noted, the FTC has been at the forefront of consumer

---

[53] MOBILE MARKETING ASSOCIATION, U.S. CONSUMER BEST PRACTICES 17 (v. 6.1 2011), *available at* http://www.mmaglobal.com/uploads/Consumer-Best-Practices.pdf.

privacy standards, so the Commission should work with the FTC throughout its process of modernizing its mobile communication privacy regulations.[54] In addition, the Commission should work with NTIA and state agencies such as the Massachusetts Office of Consumer Affairs and Business Regulations, the MDTC, and the state attorneys general nationwide. Many of these agencies are consumer protection experts, on the ground level with consumers nationwide. Insight from these agencies will help the Commission attain a regulatory framework that is beneficial to consumers and suitable to industry stakeholders.

IV. CONCLUSION.

The Commission acknowledged five years ago that consumers' privacy in their personal information on mobile phones is a vitally important issue.[55] Since then, the issue has become even more significant as not only has the use of smartphones increased generally, but consumers are increasingly using those phones for transactions that result in stored sensitive personal data on the phones and wireless networks. Accordingly, the MDTC encourages the Commission to give consumers more power over their personal information. Specifically, the MDTC recommends that the Commission require mobile carriers to obtain affirmative consent from customers before sharing their personal information with third parties; adopt rules to ensure that consumers read and understand the crux of their mobile carrier's privacy policy and their rights with respect to that policy; and require mobile carriers to delete all personal information from a mobile phone before reselling that phone to another customer. Strengthening the Commission's privacy requirements in these ways will go a long way toward putting mobile customers rightfully back in control of their personal information.

---

[54] *See* FTC Comments at 1 (offering to work with the Commission on the issue); AT&T Comments at 10; Center for Digital Democracy Comments at 11; Future of Privacy Forum Comments at 7.

[55] *2007 CPNI Order*, ¶ 72.

Respectfully submitted,

GEOFFREY G. WHY, COMMISSIONER

By: /s/ Sean M. Carroll
Paul Abbott, General Counsel
Karlen Reed, Competition Director
Sean M. Carroll, Hearing Officer

Massachusetts Department of
Telecommunications and Cable
1000 Washington Street, Suite 820
Boston, MA 02118-6500
(617) 368-1161
Sean.m.carroll@state.ma.us

July 30, 2012